



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/632,857	07/31/2003	Carey Nachenberg	20423-07776	4612

34415 7590 04/04/2007  
SYMANTEC/ FENWICK  
SILICON VALLEY CENTER  
801 CALIFORNIA STREET  
MOUNTAIN VIEW, CA 94041

EXAMINER
----------

POLTORAK, PIOTR

ART UNIT	PAPER NUMBER
----------	--------------

2134

SHORTENED STATUTORY PERIOD OF RESPONSE	NOTIFICATION DATE	DELIVERY MODE
3 MONTHS	04/04/2007	ELECTRONIC

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Notice of this Office communication was sent electronically on the above-indicated "Notification Date" and has a shortened statutory period for reply of 3 MONTHS from 04/04/2007.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptoc@fenwick.com  
bhoffman@fenwick.com  
aprice@fenwick.com

**Office Action Summary**

Application No.

10/632,857

Applicant(s)

NACHENBERG, CAREY

Examiner

Peter Poltorak

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 03 October 2005.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-32 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-32 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All   b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)  | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date <u>7/29/83/30/04, 10/3/05</u> . | 6) <input type="checkbox"/> Other: _____  |

### DETAILED ACTION

1. Claims 1-32 have been examined.

#### *Priority*

2. Acknowledgment is made of applicant's claim for priority upon commonly assigned U.S. patent application serial no. 10/612198 filed on 7/1/03. However, applicant is advised that for benefit claims under 35 U.S.C. 120, 121 or 365(c), the reference must include the relationship (i.e., continuation, divisional, or continuation-in-part) of the applications.

#### *Claim Objections*

3. Claims 1-32 are objected to because of the following informalities: the claim language lacks consistency: e.g. "said retrieval information" (claim 1) vs. "the retrieval information" (in claim 2), "real\_time" (claim 16) vs. "real-time" (claim 19), etc. Appropriate correction is required.

#### *Claim Rejections - 35 USC § 101*

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 1-11 and 13-24 are rejected under 35 U.S.C. 101 because even though the claims discuss steps of evaluating data, sent (received) in response to a retrieval command, against some rules, and based on the evaluation flagging the retrieval commands, the claimed method have no useful results. The flagged data as recited in the claim language is not further utilized in any particular way.

Including limitations similar to the limitations recited in claim 12 would overcome the 35 U.S.C. 101 rejection.

***Claim Rejections - 35 USC § 112***

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1-32 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter that applicant regards as the invention.
6. The preambles in claims 1, 32-33 do not support the bodies of the claims. Although the claim language suggests flagging code as suspicious, no limitation suggests any particular utilization of this method as pertaining to protecting computer code from malicious retrievers. Unlike claim 12, the dependent claims 2-11 and 13-31 also do not provide any limitations supporting the preamble of claim 1.
7. Claim 11 recites the term: "canonicalized command". The examiner referred to the specification in order to understand the metes and bounds of the claim language comprising this term (e.g. an example on pg. 7 lines 3-9) but was not able to ascertain the exact meaning of the term. For example it is not clear whether the command is a command that is some kind of executable code that changes a value to a "wildcard" notation, whether it is a command the value of which is changed to a wildcard value or whether it is a command comprising a wildcard value. For

Art Unit: 2134

purposes of further examination the phrase is treated as the claim language refers to a command comprising a value with multiple choices, e.g. a "wildcard" value.

8. The phrase "training phase" recited in claims 15-19 and 25-27 is not understood.

Although the specification discusses the "training phase" (e.g. pg. 16), no clear definition was found. For purposes of further examination the examiner interprets the "training phase" as phase during which a system operator (e.g. administrator) get familiar with the system (observes, updates, tests etc.). Another words the phrase is interpreted as the time during which a system operator gathers information e.g. information regarding operating of the system (e.g. maintenance, configuration, interpretation of the results etc.).

9. If examiner's interpretations are incorrect applicant should plainly clarify the desired interpretation in light of the specification.

Appropriate correction and/or clarification is required.

### ***Claim Rejections - 35 USC § 102 or 103***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Art Unit: 2134

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

10. Claims 1-8, 10, 12-13, 27 and 30-32 are rejected under 35 U.S.C. 102(e) as anticipated by or, in the alternative, under 35 U.S.C. 103(a) as obvious over Mattsson (USPN 7120933).

Mattsson's invention discloses a method of detecting intrusion in a database.

11. As per claims 1, 13 and 31-32, Mattsson discloses generating retrieval information characteristic of data sent to a retriever by the computer code (e.g. database) in response to a retrieval command issued by the retriever (col. 3 lines 38-44), accessing at least one rule using at least some of the retrieval information as an input to the at least one rule (col. 3 lines 58-65), and col. 3 line 66-col. 4 line 8 and col. 4 lines 35-59 clearly suggest flagging the retrieval command as suspicious when the at least one rule informs that the retrieval is not acceptable. As per claims 2-4, the retrieval information comprises statistical information, and a retrieval vector comprises at least one of number of rows in the retrieval, number of columns in the retrieval, number of tables in the retrieval, identification of columns in the retrieval and identification of tables in the retrieval (e.g. col. 3 lines 58-60, col. 4 lines 55-67). The cited reference also clearly indicates the presence of a plurality of retrieval commands and the statistical information comprising at least one of the statistical

characteristics specified by claim 6. The comparison disclosed by Mattsson in col. 3 line 38-col. 4 line 67 reads on an input vector containing parameterized information characteristic of the retrieval command accessing at least one rule recited by claim 7, and the limitations of claim 10 are met by col. 3 line 51-57 and col. 4 lines 16-25, and claim 12 by col. 5 lines 35-54, for example.

12. As per claim 22, col. 2 lines 27-29 and col. 5 lines 35-54 clearly suggests that the at least one rule is accessed from the group of techniques comprising real-time auditing and in-line interception, wherein at least one of: an alert is sent to a system administrator, audit log is updated, the command is not allowed to access the computer code; the command is allowed to access the computer code, but the access is limited, the command is augmented and a sender of the command is investigated is performed. As per claims 5 and 30, data (e.g. rules) in order to be accessed by computers must be kept in some form of a data structure, which reads on a table. Furthermore, in order for the data to be retrieved from a structure, the structure must exist (be pre-established). Even if a rule structure disclosed by Mattsson was not a "pure" table (e.g. a list which is a one-dimensional table, or a database which is a collection of tables) the name of the structure would not affect the functionality of the invention, especially given the fact that using tables to store rules is an obvious variations well known in the art and that an ordinary artisan would have been motivated to use them especially in light of the benefits of use of tables as evidenced by their commercial success.

Art Unit: 2134

13. Claims 1, and 31-32 are rejected under 35 U.S.C. 102(e) as anticipated by or, in the alternative, under 35 U.S.C. 103(a) as obvious over Pfleeger (Charles P. Pfleeger, "Security in computing", 2nd edition, 1996, ISBN: 0133374866).

On pages 426-433, Pfleeger discloses firewalls (e.g. screening routers) to be a mechanism that filter data based on data characteristics (e.g. intended source or destination) that is compared judged at least one rule in order to place restriction on the data, e.g. using a routing table allowing/disallowing data communication only to/from particular addresses. An ordinary artisan would recognize that in order to change status of data (e.g. mark data, as disclosed by Pfleeger, to be allowed or disallowed or, using the claim language, "acceptable" or "not acceptable") the data would have to be flagged (mark as selected).

Thus, firewalls filtering data using firewalls read on the limitations: "generating retrieval information characteristic of data sent to a retriever by the computer code in response to a retrieval command issued by the retriever, accessing at least one rule using at lest some of the retrieval information as an input to the at least one rule, and when the at least one rule informs that the retrieval is not acceptable, flagging the retrieval command as suspicious".

***Claim Rejections - 35 USC § 103***

14. Claims 9, 11, 14 and 28-29 are rejected under 35 U.S.C. 103(a) as obvious over Mattsson (USPN 7120933).

Mattson's invention has been discussed above.



Claims 9 and 11 appears to address obvious variations of searching/data retrieval techniques well known in the art of database. Claim 9 refers to searching particular fields (e.g. columns, record etc.) using more than one value at the time and claim 11 addresses "pattern search", in which rather than a specific value, wildcard value is used.

15. As per claim 11, Mattsson does not disclose a canonicalized command that is a retrieval command stripped of literal field data (as defined in the specification on pg. 7). However, using canonicalized commands that is command stripped of literal field data is old and well-known in the art of database searching (e.g. "Wild Characters", Oracle pg. 19-20). One of ordinary skill in the art at the time of applicant's invention would have been motivated to account for canonicalized commands stripped of literal field data in order to monitor/capture pattern searches.
16. As per claim 9, the examiner points out that using more than one variable as an input disclosed by Mattsson and Oracle reads on the claim limitations, since each variable could be treated as a one dimensional vector. As a result having two variables in a query comprises at least two input vectors, wherein each input vector being associated with the same retrieval command.
17. As per claim 14, Mattsson does not explicitly disclose SQL commands. However, the SQL is one of the industry-standard languages for creating, updating and, querying relational databases. Thus, incorporate SQL commands into Mattsson's invention would have been obvious variations that are well known in the art. One would have been motivated to include these commands especially in light of the

Art Unit: 2134

popularity and benefits of these commands as evidenced by their commercial success.

18. As per claim 28, Mattsson does not disclose rules being provided by a system administrator. However, the limitation is implicit. System administrators administer systems: maintain, configure etc. Updating configuration, especially configuration associated with system security is required since security threats as well as knowledge of them constantly evolves. Thus, any additional updates addressing additional known attacks (e.g. intrusion attacks) would have to involve an administrator (Note that in various system updates and configuration changes require administrative privileges).

19. As per claim 29, Mattsson does not disclose rules being provided by a vendor. However, an ordinary artisan would recognize that various systems are provided with at least default configuration (e.g. configured by a vendor) and it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to allow a vendor to provide at least one rule giving the benefit of speed and usability of setting up a new system.

20. Claims 15-26 are rejected under 35 U.S.C. 103(a) as obvious over Mattsson (USPN 7120933) in view of Sekar (USPub. 20040098617).

Mattsson discloses a system and a method as discussed above.

21. As per claim 15-16 and 18 Mattsson does not disclose previously discussed steps (e.g. developing at least one rule is developed) during a training phase.

Sekar discloses a network intrusion detection system, wherein statistical information accumulated during the training phase is used for intrusion detection rules (Sekar, [0006] and [0097]). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to develop the at least one rule disclosed by Mattsson during a training phase as disclosed by Sekar. One of ordinary skill in the art would have been motivated to perform such a modification in order to provide protection mechanism against unseen attacks.

22. As per claim 17, 22 and 27, there are inherently two obvious choices of performing any actions, in real time and not in real time, wherein each option is an obvious variation of another. Given the fact that implementation of the steps discussed above in real time or not in real time would not affect the functionality of the invention as well as that real time operations are well known in the art of computing, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement the real time training phase given the benefit of immediate feedback.

23. As per claims 20 and 23, Mattsson does not explicitly disclose using at least an API that accesses the computer code, code injection, patching, direct database integration or log file examination to extract the commands. However, using at least an API that accesses the computer code in communication involving computer processes (e.g. communicate with processes to extract particular values, e.g. commands) is well known in the art (e.g. application program interface, USPub 20030133554). It would have been obvious to one of ordinary skill in the art at the

time of applicant's invention to use at least an API that accesses the computer code, code injection, patching, direct database integration or log file examination to extract the commands given the benefit of reduced complexity.

24. As per claim 21 and 24 Mattsson does not disclose interposing a proxy or a firewall between senders of the commands and the computer code. However, Official Notice is taken that it is old and well-known practice to interpose a proxy or a firewall between a client (e.g. a requester) and a server (e.g. database. See Pfleeger for example). One of ordinary skill in the art at the time of applicant's invention would have been motivated to interpose a proxy or a firewall between senders of the commands given the benefit of additional security.

25. The limitations of claims 18 and 26 are implicit. As discussed above, Mattsson's "detection phase" includes observing retrieval commands that access the computer code, responses to the retrieval commands generated by the computer and deriving from the responses a set of retrieval information in order to identify suspicious commands. Furthermore Sekar suggests comparing a detection phase with a training phase and in paragraph (Sekar, [0097]) discloses that the configuration data are gathered during the training session, which clearly indicates that any suspicious activity would have to be reported to an administrator.

26. As per claim 25, do not disclose determining duration of performing the training phase by statistical means. However, implementation of statistical evaluations is well known in the art of science (e.g. Weisstein, "Statistics", pg. 17-26) and it would have been obvious to one of ordinary skill in the art at the time of applicant's

Art Unit: 2134

invention to determine duration of performing the training phase by statistical means given the benefit of an optimal estimate using a limited number of information.

**Conclusion**

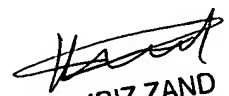
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571) 272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



3/12/07

  
KAMBIZ ZAND  
PRIMARY EXAMINER